REMARKS/ARGUMENTS

Favorable reconsideration of this application is respectfully requested.

Initially, Applicants note that with the outstanding Office Action several forms PTO-1449 were provided. One of those forms apparently is from a different application. Specifically, one of the returned forms PTO-1449 indicates an attorney docket number of 208931US0 and U.S. serial No. 09/863,383, citing as reference AA U.S. patent 4,807,416 to Kanmoch et al. That Information Disclosure Statement does not belong in the present application and is directed to a different application, i.e. is directed to application serial No. 09/863,383, which is not the present application. Removal of that Form PTO-1449 from the present application is believed to be proper.

Claims 41-80 are pending in this application. Claims 41, 42, 44, 46-62, 64, and 66-80 were rejected under 35 U.S.C. § 102(e) as anticipated by U.S. patent 6,453,419 to Flint et al. (herein "Flint"). Claims 43, 45, 63, and 65 were rejected under 35 U.S.C. § 103(a) as unpatentable over Flint and further in view of Official Notice.

Addressing the above-noted rejections, those rejections are traversed by the present response.

Initially, applicants traverse the Official Notice in the Office Action and require that prior art be cited for the positions for which Official Notice was taken.

Moreover, for the reasons now discussed applicants respectfully submit the claims as currently written clearly distinguish over the teachings, even in view of Official Notice in Flint.

Each of independent claims 41 and 61 is amended by the present response to clarify a feature recited therein. Specifically, each of claims 41 and 61 now clarifies that controlling the level of access of the computing device to the network resources using the level of security of the computer network connection that has been determined results in that:

> the computing device is allowed access to a first set of network resources based on the determined first level of security and is allowed access to a second set of network resources based on the determined second level of security.

Such claim features are believed to be fully supported by the original specification, see also for example claims 46-49 and 66-69. Claims 46-49 and 66-69 are also amended by the present response to now be consistent with the above-noted amendments to independent claims 41 and 61, respectively.

According to features clarified in the claims, if a first type of connection is made from a computing device, for example if it is an encrypted connection, that computing device can have access to a first level of network resources, such as for example access to a file server. If a second type of connection is made by the computing device, for example a non-encrypted connection, that computing device may have a more limited access to a second set of network resources, such as for example access to the Internet, e-mail, etc. Such features are now clarified in claims.

As shown in Figure 1A in the present specification as a non-limiting example, different computing devices 2, 6 can be connected to an intermediate device 10. The claimed invention has as an operation to control the access of those computing devices 2, 6 to resources on the network 12A based on how the computing devices 2, 6 connect to the intermediate device 10. With reference to Figure 2A in the present specification as a non-limiting example, if either of the computing devices 2, 6 connect to the intermediate device 10 through an encrypted connection, driver 54 is activated and a firewall setting for level 1 access is provided. In that case a high level of access to various network resources can be provided.[1] Alternatively, if no encryption is utilized for the connection between either of the computing devices 2, 6 and the intermediate device 10, the driver 56 is activated and a firewall setting for level 2 access is utilized. In that case a user may only have a limited

[1] See for example the present specification at page 6, lines 10-15.

access to resources on the network.[2] In both cases the user has access to network resources, but that access is more restricted for the level access.

In such ways, in the claimed invention, a security level of a network connection between the computing device and the intermediate device can control the level of network resources available to the computing device. The features recited in the claims are believed to clearly distinguish over the applied art.

Flint is cited with respect to the above-noted claim features. However, applicants respectfully submit that Flint does not disclose or suggest the above-noted features particularly clarified in independent claims 41 and 61. Applicants respectfully submit Flint does not disclose that with a first type of connection a computing device is allowed access to a first set of network resources and with a second type of connection the computing device is still allowed access to network resources, but to a second set of network resources. More particularly, Flint merely discloses that in one feature therein a non-encrypted connection can result in ***no access to a computer network***. The claims have a different structure in that in the claims a non-encrypted connection still gives rise to access to resources on the network, although those resources can be limited.

In further detail, Flint discloses the use of a filter 72 such as in Figure 4 therein. Flint discloses that the filter can be an encryption filter and "the encryption filter requires that a connection is encrypted with a certain level of encryption. It will be up to the user level process to verify that the requirements of the filter are met. If the requirements are not met the ***action is to deny the connection***". (Flint at column 11, lines 58-62, emphasis added).

From the above-noted disclosure it is clear that in Flint the filter is provided to merely deny a connection to a network for example if an encryption connection is not utilized.

[2] See for example the present specification at page 6, lines 15-26.

The claims have a different operation than that in Flint. In the claims connection to a network can still be provided even if a lower level connection, such as a non-encrypted connection, is utilized. However in the claims such a lower level connection, for example the non-encrypted connection, results in a different level of access to network resources, which is typically a more limited level of access.

Flint does not teach or suggest such features.

Stated another way, Flint discloses for example in Figures 1-3 the use of various firewalls 14, 34. Flint does not disclose or suggest that those firewalls determine whether connection to a network is encrypted or not. Instead, Flint uses a different type of filter to completely limit access if certain filter conditions are not met, and Flint discloses the filter conditions can require an encrypted connection. The claims require a different operation as discussed above.

In such ways, the claims as currently written are believed to distinguish over the teachings in Flint.

In view of these foregoing comments, applicants respectfully submit claims 41-80 as currently written distinguish over the applied art.

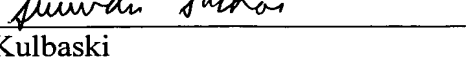
As no other issues are pending in this application, it is respectfully submitted that the present application is now in condition for allowance, and it is hereby respectfully requested that this case be passed to issue.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)
I:\ATTY\SNS\20'S\203223\203223



James J. Kulbaski
Registration No. 34,648
Surinder Sachar
Registration No. 34,423
Attorneys of Record